

## Claims

What is claimed is:

1. A method for obtaining status of public key certificate updates, the method  
5 comprising the steps of:
  - a) from time to time, providing public key certificate update subscription  
information to a server;
  - 10 b) providing an indication of a local replica of current public key certificate to the  
server while on-line with the server;
  - c) receiving an indication of updated public key certificate from the serve when the  
updated public key certificate is inconsistent with the local replica of the current public  
15 key certificate; and
  - d) while on-line, receiving an indication of newly updated public key certificate from  
the server, wherein the newly updated public key certificate relates to information of  
interest as identified in the public key certificate update subscription information.  
20
2. The method of claim 1 further comprises acknowledging receipt of the indication  
of the updated public key certificate.
3. The method of claim 1 further comprises providing the public key certificate  
25 update subscription information to include identity of at least one subscriber subject and a  
public key of the at least one subscriber subject.
4. The method of claim 1 further comprises providing the public key certificate  
update subscription information to include at least one of: signature public key certificate

5. The method of claim 1 further comprises, within step (d), receiving, as the indication of the newly updated public key certificate, at least one of: a new public key certificate for a subscriber subject, a revocation of a public key certificate of the subscriber subject, a change to the public key certificate of the subscriber subject. (encryption or signature certificate)

7. The method of claim 1 further comprises, within step (c), receiving the updated public key certificate as at least one of: updates to the current public key certificate and a message regarding updates to the current public key certificate.

8. A method for providing public key certificate updates, the method comprises the steps of:

a) from time to time, receiving a public key certificate update subscription

5 information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject;

b) monitoring public key certificate of the at least one subscriber subject; and

10

c) when a change occurs to the public key certificate, providing an indication of the change to the user.

9. The method of claim 8 further comprises:

15

receiving an indication of a user replica of the public key certificate from the user, when the user is on-line;

determining whether the user replica of the public key certificate is consistent with server  
20 replica of the public key certificate; and

when the user replica of the public key certificate is inconsistent with the server replica of the public key certificate, providing an indication of the server replica of the public key certificate to the user.

25

10. The method of claim 9 further comprises providing the indication as at least one of: the server replica of the current public key certificate and an encoded message identifying differences between the user replica of the public key certificate and the server replica of the public key certificate.

11. The method of claim 8 further comprises, within step (c), providing the indication as at least one of: an encoded message identifying the change to the public key certificate of the at least one subscriber subject.

5

12. The method of claim 8 further comprises, within step (b), monitoring the public key certificate by pulling the public key certificate of the at least one subscriber subject from a certification authority.

10 13. The method of claim 8 further comprises receiving information to change the public key certificate of the at least one subscriber subject.

14. The method of claim 8 further comprises, within step (a) receiving from an end-user or system administrator the public key certificate update subscription information.

“SECRET” E3410001

15. A method for obtaining public key certificate updates, the method comprising the steps of:

- 5 a) from time to time, providing, by a user, public key certificate update subscription information to a server, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one subscriber subject;
- 10 b) monitoring, by the server, public key certificate of the at least one subscriber subject;
- c) when a change occurs to the public key certificate, providing, by the server, an indication of the change to the user;
- 15 d) while on-line, receiving, by the user, the indication of the change; and
- e) determining, by the user, newly updated public key certificate based on the indication of the change.

20 16. The method of claim 15 further comprises:

providing, by the user, an indication of a local replica of public key certificate to the server while on-line with the server;

25 determining, by the server, whether the local replica of the public key certificate is consistent with current public key certificate of the at least one subscriber subject; and

Patent Application

by certificate  
r, an indicat  
d the current

11  
 12  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25  
 26  
 27  
 28  
 29  
 30  
 31  
 32  
 33  
 34  
 35  
 36  
 37  
 38  
 39  
 40  
 41  
 42  
 43  
 44  
 45  
 46  
 47  
 48  
 49  
 50  
 51  
 52  
 53  
 54  
 55  
 56  
 57  
 58  
 59  
 60  
 61  
 62  
 63  
 64  
 65  
 66  
 67  
 68  
 69  
 70  
 71  
 72  
 73  
 74  
 75  
 76  
 77  
 78  
 79  
 80  
 81  
 82  
 83  
 84  
 85  
 86  
 87  
 88  
 89  
 90  
 91  
 92  
 93  
 94  
 95  
 96  
 97  
 98  
 99  
 100  
 101  
 102  
 103  
 104  
 105  
 106  
 107  
 108  
 109  
 110  
 111  
 112  
 113  
 114  
 115  
 116  
 117  
 118  
 119  
 120  
 121  
 122  
 123  
 124  
 125  
 126  
 127  
 128  
 129  
 130  
 131  
 132  
 133  
 134  
 135  
 136  
 137  
 138  
 139  
 140  
 141  
 142  
 143  
 144  
 145  
 146  
 147  
 148  
 149  
 150  
 151  
 152  
 153  
 154  
 155  
 156  
 157  
 158  
 159  
 160  
 161  
 162  
 163  
 164  
 165  
 166  
 167  
 168  
 169  
 170  
 171  
 172  
 173  
 174  
 175  
 176  
 177  
 178  
 179  
 180  
 181  
 182  
 183  
 184  
 185  
 186  
 187  
 188  
 189  
 190  
 191  
 192  
 193  
 194  
 195  
 196  
 197  
 198  
 199  
 200  
 201  
 202  
 203  
 204  
 205  
 206  
 207  
 208  
 209  
 210  
 211  
 212  
 213  
 214  
 215  
 216  
 217  
 218  
 219  
 220  
 221  
 222  
 223  
 224  
 225  
 226  
 227  
 228  
 229  
 230  
 231  
 232  
 233  
 234  
 235  
 236  
 237  
 238  
 239  
 240  
 241  
 242  
 243  
 244  
 245  
 246  
 247  
 248  
 249  
 250  
 251  
 252  
 253  
 254  
 255  
 256  
 257  
 258  
 259  
 260  
 261  
 262  
 263  
 264  
 265  
 266  
 267  
 268  
 269  
 270  
 271  
 272  
 273  
 274  
 275  
 276  
 277  
 278  
 279  
 280  
 281  
 282  
 283  
 284  
 285  
 286  
 287  
 288  
 289  
 290  
 291  
 292  
 293  
 294  
 295  
 296  
 297  
 298  
 299  
 300  
 301  
 302  
 303  
 304  
 305  
 306  
 307  
 308  
 309  
 310  
 311  
 312  
 313  
 314  
 315  
 316  
 317  
 318  
 319  
 320  
 321  
 322  
 323  
 324  
 325  
 326  
 327  
 328  
 329  
 330  
 331  
 332  
 333  
 334  
 335  
 336  
 337  
 338  
 339  
 340  
 341  
 342  
 343  
 344  
 345  
 346  
 347  
 348  
 349  
 350  
 351  
 352  
 353  
 354  
 355  
 356  
 357  
 358  
 359  
 360  
 361  
 362  
 363  
 364  
 365  
 366  
 367  
 368  
 369  
 370  
 371  
 372  
 373  
 374  
 375  
 376  
 377  
 378  
 379  
 380  
 381  
 382  
 383  
 384  
 385  
 386  
 387  
 388  
 389  
 390  
 391  
 392  
 393  
 394  
 395  
 396  
 397  
 398  
 399  
 400  
 401  
 402  
 403  
 404  
 405  
 406  
 407  
 408  
 409  
 410  
 411  
 412  
 413  
 414  
 415  
 416  
 417  
 418  
 419  
 420  
 421  
 422  
 423  
 424  
 425  
 426  
 427  
 428  
 429  
 430  
 431  
 432  
 433  
 434  
 435  
 436  
 437  
 438  
 439  
 440  
 441  
 442  
 443  
 444  
 445  
 446  
 447  
 448  
 449  
 450  
 451  
 452  
 453  
 454  
 455  
 456  
 457  
 458  
 459  
 460  
 461  
 462  
 463  
 464  
 465  
 466  
 467  
 468  
 469  
 470  
 471  
 472  
 473  
 474  
 475  
 476  
 477  
 478  
 479  
 480  
 481  
 482  
 483  
 484  
 485  
 486  
 487  
 488  
 489  
 490  
 491  
 492  
 493  
 494  
 495  
 496  
 497  
 498  
 499  
 500  
 501  
 502  
 503  
 504  
 505  
 506  
 507  
 508  
 509  
 510  
 511  
 512  
 513  
 514  
 515  
 516  
 517  
 518  
 519  
 520  
 521  
 522  
 523  
 524  
 525  
 526  
 527  
 528  
 529  
 530  
 531  
 532  
 533

17. A user of secure communication system, wherein the user comprises:

processing unit; and

5 memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) from time to time, provide public key certificate update subscription information to a server; (b) provide an indication of a local replica of current public key certificate to the server while on-line with the server; (c) receive updated public key  
10 certificate from the server when the updated public key certificate is inconsistent with the local replica of the current public key certificate; and (d) while on-line, receive newly updated public key certificate from the server, wherein the newly updated public key certificate relates to information of interest as identified in the public key certificate update subscription information.

15 18. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to acknowledge receipt of the indication of the updated public key certificate.

20 19. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the public key certificate update subscription information to include identity of at least one subscriber subject and a public key of the at least one subscriber subject.

25 20. The user of claim 17 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the public key certificate update subscription information to include at least one of: signature public key certificate of at least one subscriber subject and an encryption public key certificate of the at least one subscriber subject.

5

10

15



24. A server of secure communication system, wherein the server comprises:

processing unit; and

5 memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) from time to time, receive a public key certificate update subscription information from a user, wherein the public key certificate update subscription information identifies at least one subscriber subject and a public key of the at least one  
10 subscriber subject; (b) monitor public key certificate of the at least one subscriber subject; and (c) provide an indication of a change to the user when the change occurs to the public key certificate.

15 25. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to (i) receive an indication of a user replica of the public key certificate from the user, when the user is on-line; (ii) determine whether the user replica of the public key certificate is consistent with server replica of the public key certificate; and (iii) provide an indication of the server replica of the public key certificate to the user when the user replica of the  
20 public key certificate is inconsistent with the server replica of the public key certificate.

25 26. The server of claim 25 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the indication as at least one of: the server replica of the current public key certificate and an encoded message identifying differences between the user replica of the public key certificate and the server replica of the public key certificate.

27. The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide

5

10

15

[illegible]